AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Follow up Review of Information Security Corrective Actions (05/03/00)	Information Security Office	10. A review of the COMET environment found a number of production files that could not be identified as to source or purpose.	IN PROGRESS. Information Security Office is in the process of developing and implementing appropriate processes and procedures to ensure all world-writeable files have an assigned owner and have all appropriate controls in place.
Review of Information Security (8/19/02)	Information Security Office	4.6 Hiring procedures do not require background checks for information security staff and other sensitive positions.	IN PROGRESS. Information Security Office is investigating the ability to conduct background checks for information security staff and other sensitive positions.
Review of Configuration Management (8/28/03)	Innovation Services	1.1 Information Technology Services Branch should institute a quality review process to ensure divisions' Configuration Management plans meet Information Technology Services' requirements for such plans, and monitor projects for compliance.	COMPLETE. Information Technology Services Branch instituted a quality review process to ensure divisions' Configuration Management plans meet Information Technology Services' requirements for such plans which includes monitoring projects for compliance.
Review of Internal Controls SAM 20060 (Financial Integrity and State Managers' Accountability) (12/22/03)	Information Security Office	1.1 Information Security Office should ensure that an information technology risk analysis is performed at least once every two years, and adjust the risk management practices based on the results of this analysis.	IN PROGRESS. Information Security Office is creating a methodology for the information systems risk assessment/analysis program. Target completion date is December 31, 2009.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Health Care Fund Cash Flow (5/7/04)	Employer and Member Health Services	1.2 Employer and Member Health Services should work with Information Technology Services to enhance built-in system controls that ensure all employer accounts are updated and billed properly and completely.	IN PROGRESS. Employer and Member Health Services will develop written procedures to ensure all employer accounts are updated and billed properly and completely. Target completion date is November 2009.
		1.4 Employer and Member Health Services should reconcile the billed amounts with the due amounts to ensure that it bills completely to collect all premiums due to health carriers.	IN PROGRESS. Employer and Member Health Services will continue to work with Fiscal Services to develop and implement procedures. Target completion date is November 2009.
		2.1 Employer and Member Health Services should fully implement its delinquency policy and procedures as soon as possible and work with Information Technology Services to establish system functionality allowing assessment of penalties.	IN PROGRESS. Management states there is a separate change control within the EMBARC design to establish this new system functionality. This function should be effective after PSR deploys in 2010.
		2.2 Employer and Member Health Services should ensure that detailed written procedures are developed for monitoring outstanding receivables and collection.	IN PROGRESS. Employer and Member Health Services will continue to work with Fiscal Services to develop and implement procedures. Target completion date is November 2009.
Review of Self-Funded Health Plan Administration (5/26/04)	Health Plan Administration	2.5 Health Plan Administration should request Employer and Member Health Services provide more information on the appeals log that can be used to formally analyze the data for trends and timeliness.	COMPLETE. Health Plan Administration has provided documentation to illustrate the tracking of the appeals process is adequate and that coordination with Employer and Member Health Services is being done to ensure that appeals are being tracked for critical information and timeliness.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Software Management Review (8/12/04)	Technology Services and Support	1.1 Information Technology Services Branch should ensure that staff complies with CalPERS' Information Security Practices by maintaining adequate documentation for software installed by CalPERS.	IN PROGRESS. Issues with standardizing inventory management will be resolved upon completion of the Enterprise Asset Management (EAM) effort.
		1.2 Information Technology Services Branch should ensure that the software inventory list is complete and current, based on its annual comprehensive inventory of all software installed on computer systems.	IN PROGRESS. Technology Services and Support has reviewed the Software Management Plan (SMP) but it will not be revised at this time due to the Enterprise Asset Management (EAM) project. Once the EAM project has been completed, the SMP will be updated reflecting the new solution. The SMP will be revised within the first quarter following the EAM completion date, estimated as June 30, 2008.
		4.2 Information Technology Services Branch should periodically compare software installed on CalPERS computer systems to software approved by the Information Systems Architecture Committee.	IN PROGRESS. A project to procure and install various automation tools is under way. Part of the suite of products includes a comprehensive asset tracking and reporting tool. Management will develop a practice and procedures to periodically compare and validate the Information Systems Architecture Committee approved software and the installed software to determine the accuracy and to minimize the risk of unauthorized software being installed. Target completion date is June 2009.
Data Ownership (12/21/04)	Information Security Office	1.2 Information Security Office should work with Information Technology Services to develop a complete listing of all CalPERS' data assets and follow up with business management to have ownership assigned for all data assets.	IN PROGRESS. Information Security Office will make a comparison between assets listed with the list provided by Information Technology Services. Data assets not claimed by a data owner will be reviewed for assignment of data ownership and classification. No updated target completion date was provided.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Self Funded Health Plans Cash Flow (1/11/05)	Health Plan Administration / Fiscal Services	6.1 Health Plan Administration should work with Fiscal Services to have each self funded health program product separately identified and accounted for within the Health Care Fund, so they can conduct effective cash flow planning, management, monitoring and control.	IN PROGRESS. Management states it is awaiting the impending passage of AB3041 which will enable CalPERS to use reserves from one health plan to reduce premiums in another and thus address this finding. The provision included in AB3041 will be reintroduced in the next CalPERS technical bill. The 2009 bills passed by the Legislature will be reviewed by the Governor between July and September 2009.
System Backup and Archival Process Review (5/23/05)	Technology Services and Support	2.2 Data Center should require staff to perform periodic inventories of media against the inventory lists and investigate the discrepancies. Missing media contents should be identified and reported to the Information Security Office when involving confidential information.	IN PROGRESS. Technology Services and Support will update the Information Technology Services Branch's Policy and Procedures Manual to include periodic inventories of storage media and the process to mitigate discrepancies in the inventory. The updated policies and processes will be implemented upon Technology Services and Support's management approval.
		4.1 Data Center should review the results of the restoration test performed on archived media annually to ensure that the integrity and availability of backup data are maintained.	IN PROGRESS. Technology Services and Support will update the Information Technology Services Branch's Policy and Procedures Manual to include periodic reviews of storage media test results. The updated policies and processes will be implemented upon Technology Services and Support's management approval.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Enterprise-Wide User Access Control (08/05/05)	Innovation Services / Information Security Office	2. Security Administration Services should work with Information Security Office to determine the appropriate data owner for approval of access requests to system and information assets, and modify current user access request processes to ensure that owners of systems and information assets are provided opportunities to authorize access requests.	IN PROGRESS. Information Technology Services Branch will include data owner approval processes for RIBS, CRS, and SCBA in the new TPS provisioning request system (scheduled for deployment 1st quarter 2009). These new processes will be implemented in the 1st enhancement to TPS which is scheduled to be completed by June 2009. After implementation and a suitable documentation period, ITSB/SAS will schedule meetings with the OFAS to review actions taken and request closure of this finding. Target Completion Date is September 30, 2009.
Enterprise-Wide User Access Control (08/05/05) *(continued)*	Innovation Services	6.1 Security Administration Services should coordinate with the business owners to establish a more systematic approach for effective monitoring of user account activity. Also, persons who set up access on systems should not have the responsibility of monitoring access on the same systems.	COMPLETE. Procedures have been implemented to ensure that user accounts that have been inactive for more than 45 days are deactivated for all three systems.
Review of Internal Controls SAM 20060 Financial Integrity and State Manager's Accountability (9/30/05)	Information Security Office Innovation Services	1.1 Information Security Office should complete its development of a comprehensive risk analysis program promptly. 1.2 We reviewed the Enterprise Project Management Framework and were unable to identify explicit guidelines that require systems to undergo the certification and accreditation process. Innovation Services should incorporate into the system development process explicit guidelines for security certification and processing controls considerations.	IN PROGRESS. Information Security Office will develop a comprehensive risk analysis program. Target completion date is December 31, 2009. IN PROGRESS. The Certification and Accreditation (CM) process has been developed but has not yet been tested. ITSB is currently waiting for a suitable non-PSR related project on which to do the initial test and refinement of the process. Once the C&A process has been successfully piloted, ITSB/SAS will seek executive approval for broader implementation. Target completion date is yet unknown**.**

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
PeopleSoft Review (10/26/05)	Innovation Services	3.3 We found inadequate segregation of security functions. Fiscal Services should request Security Administration Services to monitor users' activity logs.	IN PROGRESS. Information Technology Services Branch is completing the documentation of the PeopleSoft Financials security administration duties and has transferred the monitoring of user activity logs to appropriate ITSB staff to comply with segregation of duties requirements. ITSB will contact the Office of Audit Services to request a review of action taken and closure of this audit finding. Target completion date is September 30, 2009.
Data Center Move (04/26/06)	Technology Services and Support	1. Selected computer equipment did not have CalPERS asset tags. Technology Services and Support should place asset tags on all equipment belonging to CalPERS.	IN PROGRESS. Technology Services and Support has worked with Operations Support Services to replace missing asset tags. An inventory of all equipment is underway. Following the inventory, the division will work to reconcile any missing tags. The division has submitted a corrective action plan with a target completion date of July 1, 2008.
UNIX Operating System Security Review (7/31/06)	Information Security Office	1.3 CalPERS requires system services be limited to only those required for proper functioning of Unix servers. Information Security Office should periodically examine Unix servers to measure compliance with the security practice.	IN PROGRESS. Information Security Office will monitor Information Technology Services compliance with the Unix Server Security Practice.
	Unix/Linux Services	3. Unix/Linux Services copies the event log files and rotates them to a central server only accessible by administrators with privileged access; however, the log files are stored on rewritable media. Unix/Linux Services should ensure that the log messages cannot be modified by anyone gaining or having privileged access.	IN PROGRESS. CalPERS' enterprise monitoring tool is not capable of capturing all root commands and storing them in a central database that cannot be modified by the administrator (root) account; therefore a new solution tool is required. Target date to be determined.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
UNIX Operating System Security Review (7/31/06) *(continued)*	Information Security Office	8.1 Current shared ID security practice requires periodic examinations to ensure compliance with shared user IDs practice, but does not define who is responsible. Information Security should clarify the monitoring roles and responsibilities.	IN PROGRESS. Information Security Office will clarify the definitions and requirements associated with the monitoring function to ensure compliance with the shared identification practice.
		8.4 Unix system administrators do not implement and do not have sole control over the establishment of trust relationships. The Information Security Office should assess the security risks with the established trust relationships, consider needs for additional security measures, and modify security requirements if necessary.	IN PROGRESS. Information Security Office will implement a departmental security assessment methodology that will be used to assess the appropriateness of current security profile.
	Security Administration	8.6 The current access request process does not ensure that the owners approve all requests for access. Security Administration should modify the process to ensure that all requests are routed to the appropriate persons for approval.	IN PROGRESS. Management states it will work with the data owners who have applications on UNIX systems to obtain blanket approval of OS level account access for system support staff. Once the approvals are obtained and documented, management will seek to close this finding. Target completion date is June 30, 2009.
Review of Retroactive Health Benefit Terminations (4/16/07)	Employer and Member Health Services	2.1 Employer and Member Health Services should develop an active review and monitoring program to ensure that retroactive terminations, and any resulting reimbursements, are conducted accurately and in accordance with program regulations. Such a program should include identification and analysis of causes, correction, and implementation of corrective action as needed and appropriate. The monitoring program should include all segments of the population.	IN PROGRESS. Management states procedures will have to be developed to implement a review and monitoring program. Also, staffing will have to be addressed. A Budget Change Proposal for fiscal year 2009-2010 has been submitted to Department of Finance. Target completion date is January 2010.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Retroactive Health Benefit Terminations (4/16/07) *(continued)*	Employer and Member Health Services	2.2 Employer and Member Health Services should work with the Office of Health Policy and Program Support to ensure COMET correctly limits reimbursements in accordance with program regulations.	IN PROGRESS. Management states procedures will have to be developed to implement a review and monitoring program. Also, staffing will have to be addressed. A Budget Change Proposal for fiscal year 2009-2010 has been submitted to Department of Finance. Target completion date is January 2010.
		2.5 Pending reimbursements being held due to the Medicare overpayment component should be promptly cleared.	COMPLETE. Employer and Member Health Services has cleared the pending reimbursement list and fully addressed the finding.
Operational Recovery Planning Process (7/23/07)	Information Technology Services Branch	2.1 Current policy does not require all staff to attend an annual Disaster Recovery Training seminar. Since August 2004, staff levels for the Information Technology Services stand at more than 480 employees. However, only 72 employees attended a seminar in 2005 and 88 in 2006.	IN PROGRESS. The Disaster Recovery Unit is currently updating training materials and is scheduled to resume Disaster Recovery (DR) training in October 2008. Target Completion Date - July 7, 2009.
		4.1 The Operational Recovery Plan has areas of incomplete and/or outdated information. Telephone and pager numbers are not listed for selected staff, recovery locations mentioned are no longer used, and list information between business critical functions, applications, and information technology requirements are not adequately illustrated.	IN PROGRESS. All Disaster Recovery plans are currently being updated. These plans are used to populate the Operational Recovery Plan (ORP). There are 33 plans to update and this new information will be part of the new ORP, due to the State Office of Information Security and Privacy Protection (OISPP) on January 15, 2009. Target completion date is March 30, 2009.
	Technology Services and Support	4.2 CalPERS has two designations with very similar recovery responsibilities assigned to two different positions within the Technology Services and Support Division.	IN PROGRESS. The Operational Recovery Plan has been updated to reflect the inconsistency with the two designations. However, the changes are not reflected in CalPERS' Business Continuity Plan. The Disaster Recovery Unit will work with Operation Support Services Division to update the BCP. Target completion date is February 28, 2009.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Operational Recovery Planning Process (7/23/07) *(continued)*	Information Technology Services Branch	4.3 CalPERS has an inter-agency agreement with the Department of Technology Services for recovery services from IBM. The current contract expired on 6/30/06 and a proposed contract was still being reviewed by the end of March 2007.	IN PROGRESS. The current Inter-Agency Agreement between CalPERS and the Department of Technology Services (DTS) expires June 30, 2009; however, the agreement does not provide enough details regarding the type of recovery services that is to be provided to CalPERS in a disaster situation. The Disaster Recovery Unit is currently working with DTS to update the statement of work language to be more specific about the recovery services being provided to CalPERS.
		5.1 Technology Services and Support's Disaster Recovery Unit is not always made aware of production environment changes. Currently, a representative from the Disaster Recovery Unit is not required to sign the Change Request form acknowledging that it has been made aware of changes.	IN PROGRESS. Information Technology Services Branch's Project Management Office added Disaster Recovery tasks to all project templates. The Change Control Policies and Procedures are currently being updated to reflect communication to the DRU of all changes made to the production environment. In addition, the new form will include check boxes to determine if there is an impact to the Disaster Recovery plan. Target completion date is March 30, 2009.
		5.2 The Disaster Recovery Policy does not specifically define the frequency that the Plan should be tested or the extent of testing required.	IN PROGRESS. Information Technology Services Branch is taking the appropriate action to update its Disaster Recovery Policies and Procedures manual to state the frequency that the Disaster Recovery testing should occur, as well as state the extent of testing required. Target completion date is July 7, 2009.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Operational Recovery Planning Process (7/23/07) *(continued)*	Information Technology Services Branch	5.3 In June 2006, a full recovery test was scheduled, but was stopped before full recovery was achieved. A report summarizing weaknesses identified was not finalized. The Operational Recovery Plan was still pending revision as of May 2007.	IN PROGRESS. The 2008 Operational Recovery Plan (ORP) is updated to reflect changes to the old recovery strategy. The Information Technology Services Branch (ITSB) Disaster Recovery Policies and Procedures manual will be updated to reflect that ORP testing is completed annually. The current recovery strategy was reviewed during the Stanfield Study. The study is complete and ITSB Management is educating CalPERS Executives on the outcome of the study. A decision on future direction will be made by the CalPERS Board. Target completion date is July 7, 2009.
Global Public Markets External Investment Manager Review (Barclays) (8/2/07)	Investment Office	8.1 For future agreements between CalPERS and Barclays Global Investors, as well as other managers, the Investment Office should work with Contract Management to develop appropriate contract language to address the disaster recovery capabilities of the external manager.	COMPLETE. Operations Support Services has drafted contract language and a series of inquiries to be included in the Request for Proposal that will address disaster recovery capabilities.
Review of the Employer Reporting Process (10/19/07)	Employer Services	3.3 Employer Services does not monitor the due dates for employer payroll to ensure that requests for extensions are received ten days prior to the payroll due date. The current system does not have the capability and no manual processes were developed.	COMPLETE. Employer Services has created a procedure to monitor Payroll Extension Requests for current process (pre-PSR). This procedure was approved by the Payroll Manager and Assistant Division Chief. We also reviewed PSR specifications to ensure this finding is covered in the new system.
Alternative Investment Management External Partner Review - 2006 (11/13/07)	Investment Office	5.1 The General Partner has a disaster recovery plan to safeguard the partnership's investment information. However, the Limited Partnership Agreement does not include a provision requiring a disaster recovery plan.	COMPLETE. Alternative Investment Management developed a procedures manual that detail processes and senior management approvals if a prospective partner does not have a disaster recovery plan. Most partners do have disaster recovery plans, and to date, Alternative Investment Management has not had to seek approval for any exceptions.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07)	Information Security Office	1.1 The Separation of Duties Practice contains broad separation of duties requirements. The job categories are not defined, nor has CalPERS adopted a formal set of definitions.	IN PROGRESS. Information Security Office will revise the Separation of Duties Practice to define job categories that require separation.
	Technology Services and Support	1.3 Information Technology Services Security Administration monitors wireless activity at CalPERS. Its monitoring does not cover all CalPERS locations. Lincoln Plaza East, Regional Offices, and the Emergency Operations Center are not monitored.	IN PROGRESS. Information Technology Services Branch has worked with Colliers to procure and deploy additional AirDefense sensors for the entire Lincoln Plaza campus, Regional Offices and the Emergency Operations Center. ITSB/SAS has developed and implemented wireless activity monitoring procedures and begun to monitor wireless activities at all CaIPERS locations. ITSB/SAS will schedule meetings with the Office of Audit Services to review actions taken and request closure of this finding during the 1st quarter of 2009. Target completion date is March 31, 2009.
	Information Security Office	1.4 Neither Information Technology Services Branch nor the Information Security Office performs a periodic range scan to ensure the boundary of the wireless network has not been altered.	IN PROGRESS. Information Technology Services Branch has augmented and documented its current wireless monitoring procedures to include wireless range scanning and signal strength validation of authorized CaIPERS access points. Following two or more successful scanning cycles and completion of the documentation, ITSB/SAS will schedule meetings with the Office of Audit Services to review actions taken and request closure of this finding. Target completion date is September 30, 2009.
	Information Technology Services Branch	1.5 Password configuration enforcement was reviewed for ACES, COMET, CRS, PA Billing, RIBS, and SCBA systems. It was noted that the systems' configurations do not always comply with the requirements specified in the security practice. The degree and area of noncompliance varies by system.	IN PROGRESS. Information Technology Services Branch continues to work on password configuration enforcement for these systems/applications.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07) *(continued)*	Information Security Office	1.6 Information Security Office does not currently monitor password compliance.	IN PROGRESS. Information Security Office will implement automated tools to measure compliance with password requirements.
	Information Technology Services Branch	1.7 Office of Audit Services observed instances of login IDs failing to comply with the Identity Authentication Practice.	IN PROGRESS. Information Technology Services Branch is coordinating with ISOF to conduct password scanning on CorP, AceP, CRS, RIBS, SCBA, PA Billing and ACES in 2nd quarter 2009. Once the scan results are in, ITSB will conduct a risk assessment to determine the security risks posed by the results, and will work to address any areas of non-compliance or obtain variances from ISOF, where appropriate. Target completion date is September 2009.
		1.8 Information Technology Services Branch is in the process of defining security standards. It keeps a list of Microsoft servers, but the list was not current.	IN PROGRESS. Windows and Network Directory Services developed a draft security policy and security standards for servers managed by it in 2002 and 2003 respectively. These standards will be finalized by management. Windows and Network Directory Services maintain an inventory database of all servers it manages and maintains.
	Information Security Office	1.9 We reviewed a sample of six systems and did not observe evidence that management reviewed system logs for changes made to user profiles by security administrators.	IN PROGRESS. Information Security Office will modify the Event Logs Practice to require periodic review of all event logs, including those that record changes to user profiles by the Information Security Office.
	Information Technology Services Branch	1.10 The only portable devices being encrypted now are laptop computers. Other portable computing devices such as Personal Digital Assistants (PDAs) are not encrypted.	IN PROGRESS. Technology Services and Support Division/ Enterprise Desktop Customer Services are in the process of developing a strategy and augmenting staffing levels to address PDA encryption. This will include coordinating with Information Technology Administration Division to develop and implement policy and procedure to ensure that all portable devices containing personal, sensitive, or confidential data are encrypted.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07) *(continued)*	Operations Support Services	1.11 Of 1,055 laptops identified on Operations Support Services Division's inventory records, 637 were not on the Enterprise Desktop Computer Services' list of laptops with installed encryption software. We attempted to test 30 of the 637 laptops for proper encryption, but were unable to locate 14 of the 30 laptops.	IN PROGRESS. Operations Support Services conducted a physical inventory of all laptops and is working with Information Technology Service Branch to ensure that encryption is installed on all laptops containing CalPERS data.
	Information Security Office	1.12 The Software Licensing Practice does not require that software be only acquired from reliable and safe sources.	IN PROGRESS. The Information Security Office will add this requirement to the Software Licensing Practice.
	Technology Services and Support	1.13 Data owners are not consistently part of the remote access approval process. Out of 11 systems' data owners contacted, only four indicated they have knowledge that staff is able to remotely access data. Only two of 11 systems' data owners are involved in the remote access approval process.	IN PROGRESS. Technology Services Branch's procedures have been revised to include data owner approval for designated systems prior to granting remote access. Additionally, if the request is for an employee of the Fiscal Services Division, access to SideStreet is also checked, and if found, approval is requested from the data owner. After the new process has been utilized, Information Technology Services Branch will contact the Office of Audit Services to request a review of actions taken and closure of this finding. Target completion date March 2009.
	Information Security Office	1.14 Data owner responsibilities are defined, but not all are implemented. Out of 11 systems' data owners that were contacted, seven indicated that they are not currently performing a periodic review of user accounts to ensure that access granted remains appropriate.	IN PROGRESS. Information Security Office will provide annual notification to data owners of their responsibilities, including the responsibility to monitor access authorizations.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07) *(continued)*	Information Security Office	1.15 A sample of 30 termination/transfer requests were tested. Nineteen requests were not submitted five days or more before the effective date. Ten of the 30 requests were not processed within 10 days from the request or effective date, whichever was later.	IN PROGRESS. Information Security Office distributed instructions to all managers, supervisors and system administrators describing the requirements for timely termination of user accounts that are no longer needed in November 2007. Similar notifications will be sent periodically in the future**.**
		1.16 Written procedures have not been established to ensure consistent and proper handling and reporting of security incidents.	IN PROGRESS. Information Security Office will develop internal procedures to document the process for incident reporting.
		1.17 Current external reporting requirements contained within the Information Security Incidents Practice do not fully incorporate or reference current external reporting requirements contained in SAM §4845. Potential security incidents requiring external reporting may not be properly and timely reported.	IN PROGRESS. Information Security Office will modify the Security Incidents Practice to refer to the external reporting requirements as defined in the State Administrative Manual §4845.
	Operations Support Services	1.18 Operations Support Services and Building Management have not fully implemented policies and procedures for requesting, establishing, modifying, terminating, and controlling temporary building access badges.	COMPLETE. Operations Support Services established implementation policies and procedures for controlling temporary building card badges, and will account for or disable temporary access badges.
		4.2 The control log of Blue Card users is not kept current. This is a necessary internal control to ensure accountability.	COMPLETE. Operations Support Services has established a process to keep track of the Blue Cards on a going forward basis. In addition, the DGS master list of Blue Cards is reconciled against the internal CalPERS list, and a process for cancelling Blue Cards not accounted for, damaged, or destroyed is established.
		4.3 Periodic inventories of the Blue Card are not performed. This is a necessary internal control to ensure accountability.	COMPLETE. Operations Support Services has established a process for integrating the periodic physical inventory and updating the data into the physical control log.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07) *(continued)*	Operations Support Services	4.4 There are no reconciliations between CalPERS' Blue Card control log and Department of General Services' Master List as prescribed in the Office of Fleet Administration Handbook.	COMPLETE. Based on the actions taken by Operations Support Services and on our review of the documents provided, we determined that this finding should be classified as completed. Operations Support Services is reconciling the Blue Card inventories at CalPERS with DGS' Master list.
	Fiscal Services	5.3 Review of the general checking reconciliations revealed that the most recently completed reconciliation as of June 2007 was February 2007. As of June 2007, the individual who conducted the reconciliations transferred to a different unit and as of our fieldwork, no one was assigned to the general checking reconciliation.	COMPLETE. Fiscal Services has effectively implemented a log to track and monitor the status of bank reconciliations and the actual completion of bank reconciliations within the 30 day limit required by SAM Section 7901. It has amended procedures to include signature approvals for amended bank reconciliations.
		6.6 Fiscal Services performs monthly reconciliations for Revolving Fund Cash Book. Although errors are identified as reconciling items that require correcting entries, they are not resolved timely.	COMPLETE. Fiscal Services researched and corrected older outstanding reconciling items, and is keeping current on the monthly reconciliations.
		6.8 A review of the Benefit Revolving Fund Aging Report for January 2007 revealed numerous payables and receivables that are aged over 90 days.	COMPLETE. Fiscal Services, in collaboration with Benefit Services, has established a process for clearing accounts from the Benefit Revolving Fund that are greater than 90 days old and has made numerous corrections to clear the aged items.
	Human Resources Services	7.6 Human Resources Services did not review the employee leave balance compliance with the minimum leave balance requirements for direct deposit for the period of July 1, 2006 to September 30, 2006.	COMPLETE. Human Resources Services has demonstrated that there is a process in placed for notifying employees regarding their direct deposit eligibility and that the process is being successfully implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Internal Controls – Financial Integrity and State Managers Accountability Act (FISMA) (12/21/07) *(continued)*	Operations Support Services	8.1 Information technology equipment is not consistently assigned to the user division within the PeopleSoft Asset Management module. Often times, Information Technology Services Branch remains as the assigned user of the property after IT equipment has been delivered to the requesting division.	IN PROGRESS. Operations Support Services has a project for an asset management program in progress. The systems should be implemented by May 2009 pending needed data cleanup. Office of Audit Services has a representative on this project.
		8.3 During discussion with various division property custodians, we found the on-line instructions were not comprehensive enough to properly inform them of the detail process needed to acquire or dispose of assets within their unit.	COMPLETE. Property Controllers will conduct bi-monthly meetings with property custodians to provide a clear understanding of their duties in order to perform accurately and consistently. Operations Support Services is also completing procedures for property custodians to follow.
		8.4 Operations Support Services has not made a physical count of all CalPERS fixed assets and has not reconciled it to the accounting records since November 2002. Many of the sampled assets could not be located even with the assistance of the property custodians.	COMPLETE. Management states the physical inventory has been completed as of June 2008, and adjustments to PeopleSoft were made so book agrees with the physical counts. Operations Support Services plans to continue physical inventories on an ongoing basis.
State Street Client Specific Review (12/21/07*)*	Investment Office	2.1 Recalculations were done for 48 monthly dynamic benchmarks presented within the Chief Investment Officer's performance reports to check for completeness and accuracy. Four portfolio benchmark changes were not updated resulting in an understatement of three composite fund benchmarks. One performance benchmark was overstated by three basis points and two composite funds were not included in the Chief Investment Officer's report.	COMPLETE. Investment Office and State Street researched and determined the errors noted had neither material impact to the CIO report, nor impact on a portfolio that was used to determine staff performance award. Investment Office is implementing a new tool, Index Builder, to help ensure such errors do not go undetected in the future.
		2.2 Recalculating benchmarks using State Street's web-based system could present a limitation to the Investment Office given the time and effort needed to compile and generate these reports.	COMPLETE. Investment Office now has State Street Index Builder tool to enable automatic recalculation of benchmarks.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Configuration Management Review (5/30/08)	Information Technology Services Branch	1.1 Information Technology Services Branch has not established a governing policy and procedural framework for a configuration management program.	CONCUR. Currently, Information Technology Services' configuration management practices are decentralized and disparate throughout the branch. However, utilizing IT industry standards and best practices, and the IT Infrastructure Library framework, ITSB has an effort underway that will implement standardized policies and procedures and establish governance for an enterprise-wide and centralized configuration management program with complementary automation tools. Target implementation date is 2nd quarter, 2009.
		2.1 Information Technology Services Branch should establish policies and procedures outlining the scope of configuration items, attributes to be recorded, and baselines to be established.	CONCUR. See Response to Finding 1.1 above.
		3.1 Information Technology Services Branch has not established a single repository or centrally coordinated approach to maintain data on configuration items.	CONCUR. See Response to Finding 1.1 above..
		4.1 Information Technology Services Branch has not established branch-wide processes for the management of data on configuration items.	CONCUR. See Response to Finding 1.1 above
		5.1 Information Technology Services Branch does not maintain branch-wide policies on access controls to configuration data repositories.	CONCUR. See Response to Finding 1.1 above.
		5.2 Staff have the ability to access and later the configuration data maintained on a spreadsheet. No written procedures are available to communication restricted access to appropriately authorized staff.	CONCUR. See Response to Finding 1.1 above.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Configuration Management Review (5/30/08) *(continued*	Information Technology Services Branch	5.3 DataCom did not provide procedures that outline processes to ensure access to configuration data in their repository is restricted to appropriately authorized staff.	CONCUR. See Response to Finding 1.1 above.
		6.1 Information Technology Services Branch has not established a governing policy and procedural framework for a configuration management program that includes periodic configuration status verification.	CONCUR. See Response to Finding 1.1 above.
		6.2 Historical records for configuration items are not maintained to enable reconciliation among baseline, authorized changes and actual configurations.	CONCUR. See Response to Finding 1.1 above
		6.3 Information Technology Services Branch does not maintain historical records for installed configuration items to enable reconciliation of baseline, authorized changes and actual configurations.	CONCUR. See Response to Finding 1.1 above.
		7.1 Information Technology Services Branch does not maintain policies at the branch level for controlling access to software libraries.	CONCUR. See Response to Finding 1.1 above.
		7.2 Access and sign-out logs for admission to physical software libraries are not reviewed and an authorized staff access list is not maintained.	CONCUR. See Response to Finding 1.1 above.
		7.3 The DataCom unit does not maintain or review an authorized staff access list and access logs for access to logical software libraries.	CONCUR. See Response to Finding 1.1 above.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Building Manager's Administrative Billings (6/23/08)	Operations Support Services	1.1 Expenses that are to be charged to the building manager per CalPERS' contract were erroneously billed to the CalPERS building account, the payments made were incorrect, and there was inadequate supporting documentation for these charges.	CONCUR. Operations Support Services will work with the Building Management Office to develop a procedure to review and verify all invoices to ensure they are billed to the appropriate account, the invoices are for building related items, mathematically correct, and have supporting documentation. In addition, the building manager will stamp reimbursement forms to indicate "Corporate Expense, Do Not Pay From Building Account" to prevent charging errors.
		2.1 Operations Support Services does not ensure that the Colliers accounting office has proper segregation of duties relating to approval and disbursements related to invoices, checks, transfers of funds and bank reconciliations.	CONCUR. Operations Support Services will work with the Building Management Office to update the separation of duties procedures to require Colliers to separate the cash disbursement duties. Colliers has revised its process so that the Senior Accountant no longer has the authority to transfer funds. This is now done by the controller and an accountant. Colliers' policy now states than any one individual cannot be the first and second signor.
		3.1 No surprise counts of petty cash were conducted nor is a log sheet used to track and summarize the petty cash disbursements and the replenishments as per policies and procedures.	CONCUR. Operations Support Services will work with the Building Management Office to develop a log sheet similar to the one used by Fiscal Services to track and summarize all petty cash disbursements and replenishments. Operations Support Services will also conduct periodic surprise counts of the petty cash to ensure proper documentation is maintained for the handling of all petty cash transactions.
		5.1 Bank reconciliations for the Parking account did not indicate the data that the reconciliations were signed off by the reviewer.	CONCUR. Operations Support Services will work with the Building Management Office to ensure that staff are trained on the statement reconciliation procedures.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS - INTERNAL AUDITS
(PRIOR YEAR REPORTS WITH CURRENT YEAR UPDATES)
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Review of Building Manager's Administrative Billings(6/23/08) (*continued)*	Operations Support Services	6.1 The Colliers contract does not stipulate the type of bond required for bond covering requirements.	CONCUR. Operations Support Services will determine the bonding required and work with the Building Management Office to modify the contract to include the type of bond required for Colliers staff that handle and have access to CalPERS funds.
		6.2 The "General Liability" and the "Primary Umbrella Liability" insurance certificates revealed that the coverage amounts were reflected in Canadian dollars whereas they should be stated in US dollars.	CONCUR. Operations Support Services will keep a copy of all required bonding and insurance policies and review this information annually to ensure proper coverage and conditions comply with the contract.